Memo of Meeting

Date: September 6, 2001
1350 Piccard Drive, Rockville, Maryland

Representing Ionics Instruments, Boulder, CO:

Mr. William McHale, Applications Manager
Mr. Greg Krishner, Software Engineering Manager
Mr. David M. Wayne, Global Accounts

Representing the Food and Drug Administration:

Mr. Paul J. Motise, Consumer Safety Officer, Office of Enforcement
Dr. Charles Snipes, Ph.D., Compliance Officer, Center for Drug Evaluation and Research
Dr. James McCormack, Ph.D., Consumer Safety Officer, Office of Enforcement
Mr. Tom Chin, Consumer Safety Officer, Office of Enforcement

The meeting was held at the request of the Ionics Instruments representatives, to discuss their firm's lab instrumentation in the context of 21 CFR Part 11. At the start of the meeting we explained that FDA doesn't formally evaluate products or services that enable regulated companies to comply with FDA requirements and that our comments should be taken in that context.

During the meeting our discussions focused mainly on the software and security features of the firm's total organic compounds analyzer, as used by the firm's pharmaceutical customers. The representatives explained that over the past 18 months those firms have shown an increased focus on how the electronic records produced by the analyzer meets part 11 requirements. The analyzer can function as a stand-alone unit or can be integrated into a laboratory information management system.

In our discussions we explained FDA's part 11 enforcement policy, as contained in our compliance policy guide 160.850. We commented that regulatory actions depended upon the nature and extent of the violations, the impact on product quality and data integrity, a firm's history, and the adequacy of a firm's corrective action plan (along with the progress a firm has made in meeting the plan.)

In response to the representative's questions, we discussed various technical provisions of part 11 and how they might be engineered into a stand-alone device or, to overcome limitations of software embedded into such devices, integrated into a wider system. We advised that FDA is in the process of developing a series of guidance documents that would help industry implement the regulation.

With respect to transaction safeguards to report security breaches to appropriate individuals in an urgent and immediate manner, we commented that an e-mail notification might satisfy this provision. We also commented that a deferred review of a log of such events would not have the immediacy needed.

We discussed password controls and the importance of ensuring that no two combinations of id code/password would be the same.

We discussed exporting instrument calibration information to an electronic record external to the lab instrument and how that could be engineered to meet part 11 requirements. We commented that controls to ensure application of robust passwords (e.g., length, composition and re-use limits) could also be implemented outside of the instrument itself.

During the meeting we discussed the firm's validation efforts. One of the firm's customers had requested a validation certificate – in response the firm explained to the customer that the nature of validation entailed on-site evaluation/testing factors that made issuance of such a certificate moot. The firm provides installation and operational qualification services to its customers and is amenable to, and has undergone, audits of its software development activities.

Regarding the generation of electronic copies of electronic records suitable for FDA review, the representatives indicated that a proprietary file viewer would be needed to read the instrument files and that such a viewer would be made available to FDA investigators. We commented that such an arrangement might not meet the part 11 requirement and that exporting to a file format we can process using our own software would more assuredly conform.

We also discussed the firm's DataGuard autoanalyzer software and the representatives showed us the program on their laptop computers. We noted that human readable manifestations of electronic signatures (based on id codes and passwords) included the signer's printed name, the date and time of signing and what the signature meant.

The autoanalyzer software also implements audit trails which record the operators name and identification number, the date/time of the trailed event, the type of event, any prior values for altered data fields, and a user comments field. We said that the comments field should not be part of the audit trail because the operator should not be able to write to the audit trail, and in highly secure environments should not be able to read the audit trail. We suggested that if it was important to preserve operator comments that the comments be captured to the trailed record itself. The representatives said that end user read access to the audit trail was configurable in the software.

The representatives asked about the intent behind the part 11 device checks provision. We explained that device checks would be appropriate in those

instances when certain commands or information, as a matter of security and authentication, must only have originated from a given computing device (e.g., workstation.) In those cases the system receiving the command or information would confirm the identity of the issuing computing system.

With respect to archiving, we discussed the need to preserve the electronic records in a form that retained the ability the process the electronic record's information, and authenticate the record's signatures.

The representatives commented that information could emerge from their instrument from any of several different ports (channels.) They asked if part 11 addressed this matter. We advised that part 11 only addressed this in the general requirements for system validation and record accuracy and completeness. We commented that different firms may have systems that, by their nature and use, made one type of port preferable over others.

We discussed how certain of the firm's part 11 functions could be configured to be turned off upon first delivery. We suggested that the default setting be that the features are turned on and that the disabling feature be delivered in a deactivated state. We commented that mainstream standards in e-commerce and e-government were broadly echoing part 11 technical requirements and that the demand for the features should therefore increase.

The representatives asked if durable media was part of the definition of electronic record. We said that it was not. We commented that people were using devices that recorded information to media such as flash memory and that as long as a human readable form of the electronic record could be generated the durability of the media was not a factor. We advised that this approach was consistent with the Electronic Signatures In Global and National Commerce Act.

The meeting lasted about two hours.

cc:
HFA-224
FDA attendees
Part 11 Guidance Dockets
doc id: MemoOfMeetingIonics090601.doc
P. Motise 9/7/01